TITLE OF THE INVENTION

Method of and System for Making Purchases Over a Computer Network

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to a method of and system for making purchases over a computer network and, more particularly, to a method of and system for making purchases of goods and services over the Internet or other non-secure computer network using an automated-teller-machine (ATM) card, debit card or any other card which may require a valid personal-identification-number (PIN) for transaction authorization.

2. Description of the Prior Art

The use of personal computers by consumers to purchase goods and services over the Internet via the World Wide Web and e-mail has become very popular in recent years and constitutes an ever-increasing part of the economy. In making a purchase over the Internet, the typical consumer uses a credit card or ATM card. After making his purchase selection, the consumer transmits his card information over the Internet to the on-line merchant. The on-line merchant then contacts the issuing bank to verify the card information and obtain authorization to complete the transaction. Depending on the response from the bank, the on-line merchant either accepts or rejects the purchase.

Because the Internet is a non-secure (i.e., public) network, there is a danger that the consumer's credit card or ATM card information will be intercepted by a third party. If that third party is dishonest, he can make illegal charges to the credit card or, in the case of an

ATM card, remove money directly from the consumer's bank account. In recent years, numerous approaches have been implemented to reduce this security risk. The most popular approach has been sophisticated encryption techniques which render the credit card or ATM card data virtually unreadable to third parties, such as 128-bit secure-sockets-layer (SSL) encryption.

When making purchases over the Internet using an ATM card, however, security considerations take on an added importance because, unlike with transactions at ATM machines, PINs are presently not used in ATM transactions on the Internet. Thus, should the ATM card number fall into the hands of an unscrupulous third party, the card-holder's entire bank account can be wiped out through fraudulent Internet transactions.

One way to overcome this problem is to require the use of PINs in ATM transactions on the Internet. This has not been possible to date, however, because on-line merchants do not have the ability to verify PINs. Additionally, it is not desirable to provide the on-line merchant with both the ATM card number and the corresponding PIN since unscrupulous employees of the on-line merchant can use the PIN to illegally access the card-holder's bank account and withdraw money therefrom.

Accordingly, it is an object of the present invention to provide a new method of and system for making purchases over the Internet using an ATM card wherein a valid PIN is required in order to obtain authorization for a given transaction. It is another object of the present invention to provide a new method of and system for making purchases over the Internet using an ATM card wherein a valid PIN is required in order to obtain authorization for a given transaction, and wherein the PIN is not supplied to the on-line merchant.

SUMMARY OF THE INVENTION

In accordance with a first aspect of the present invention, a method of making purchases over a non-secure computer network using an ATM card is provided. In accordance with said method, a consumer transmits his ATM card number over the network to an on-line merchant. The on-line merchant then forwards the ATM card number to a third party contractor, such as a bank, that will oversee and authorize the transaction. Simultaneously or thereafter, the consumer transmits his PIN over the network to the third party contractor, bypassing the on-line merchant. Having both the ATM card number and the PIN, the third party contractor verifies that the ATM card number and PIN are correct, checks for sufficiency of funds, and either authorizes or denies the transaction. The authorization or denial is communicated to the on-line merchant over the network, who either completes or rejects the purchase and so notifies the consumer.

In accordance with a second aspect of the present invention, a system for making purchases over a non-secure computer network using an ATM card is provided. The system includes first, second and third computers connected to a computer network. The first computer transmits the consumer's ATM card number over the network to the second computer, which is operated by or for the on-line merchant. The second computer forwards the ATM card number over the network to the third computer, which is operated by or for the third party contractor. Simultaneously or thereafter, the first computer transmits the consumer's PIN over the network to the third computer, bypassing the second computer. The third computer then verifies that the ATM card number and PIN are correct and that there are sufficient funds in the bank account to cover the transaction amount. The third computer then transmits the results of the verification procedure to the second computer, which

forwards the results to the first computer. Depending on the verification results, the purchase is either completed or rejected.

The present invention will now be described in detail, with frequent reference being made to the drawings identified below.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings:

figure 1 is a schematic diagram of the system in accordance with the present invention;

figure 2 is a flow chart which illustrates how the system of figure 1 operates;

figure 3 shows a possible graphical user interface which can be used to enable the consumer to enter and transmit his PIN to the third party contractor;

figure 4 is a diagram which summarizes the present invention;

figures 5(a) - (d) show a computer program which can be used to format the data package sent from the second computer to the third computer in ISO 8583 format; and

figures 6(a) - (f) show a computer program which can be used by the third computer to synchronize the data packages received from the first and second computers.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The system 10 in accordance with the present invention is schematically shown in figure 1. The system 10 includes a first computer 12 at a consumer location 14, a second computer 16 at an on-line merchant location 18, and a third computer 20 at a third party contractor location 22. The three computers 12, 16, 20 are connected together over a

computer network 24 which, for purposes of this discussion, is the Internet, although the present invention may be practiced on any computer network. As those of ordinary skill in the art know, the Internet 24 is a complex and amorphous computer network that comprises thousands of nodes and components and over which signals are transmitted by telephone lines, satellites and optical fibers.

The first computer 12, which will generally be located at the consumer's home or business (consumer location 14), will typically be a conventional personal computer (PC) that includes a chassis that houses a central processing unit (CPU) and supporting circuitry, as well as a floppy drive, a hard drive and an internal modem. Connected to the CPU through the chassis are a keyboard, a mouse and a monitor. The keyboard and mouse are used by the consumer to control the operation of the first computer 12 and to input information into the first computer 12. The first computer 12 will usually be coupled to the Internet via a telephone line connected to the modem, although the computer can be connected to the Internet via a high speed data transmission line. The consumer will typically connect to the Internet using an Internet service provider, such as Erols™ or America OnLine™, but may have a direct connection to the Internet.

Although a conventional PC will typically be used by the consumer, the consumer may use any type of computer that can be connected to the Internet, including a work station on a local area network, and any operating system. The particular details of the first computer 12 are largely irrelevant to the present invention. The first computer 12 merely serves as a convenient interface for the consumer to place orders for goods and services over the Internet.

Next shown in figure 1 is the second computer 16 which is located at the on-line merchant location 18. The second computer 16 will preferably be a more powerful machine than a personal computer, such as a workstation, although a personal computer may also be used by the on-line merchant. Again, the particular details of the second computer 16 are largely irrelevant to the present invention.

Typically, the second computer 16 will be a Web server (a computer that provides direct access to the World Wide Web on the Internet and includes the necessary hardware, operating system, Web server software, TCP/IP protocols and Web site content) owned and operated by the on-line merchant or by an Internet service provider with whom the on-line merchant has contracted. For purposes of this discussion, the on-line merchant location 18 refers to the location of the second computer 16, and not necessarily the actual physical location of the on-line merchant.

Preferably, the second computer 16 will be running Windows NT™ 4.0, using Internet Information Server™ 4.0 and Commerce Server™ 3.0. The CPU of the second computer 16 must have acceptable power and should have at least 64 megabytes of RAM.

The second computer 16 will typically have an on-line catalog in memory which can be accessed and browsed by the consumer over the Internet 24 through an appropriate graphical use interface (GUI) supplied by the on-line merchant.

Next shown in figure 1 is the third computer 20 which is located at the third party contractor location 22. The third party contractor is an independent, insured organization, such as a bank, that has contracted with the on-line merchant to provide ATM services. Although the third computer 20 can be a personal computer, as with the second computer 16 it will preferably be a much more powerful machine, such as a workstation. The third

computer 20 is likewise preferably a Web server owned and operated by the third party contractor or by an Internet service provider with whom the third party contractor has contracted. The third party contractor location 22 refers to the location of the third computer 20 and not necessarily the actual physical location of the third party contractor. As with the first and second computers 12, 16, the particular details of the third computer 20 are largely irrelevant to the present invention, so long as the third computer 20 is capable of performing the functions described herein. Preferably, the third computer is Compaq ProLiant™ server running at 500 MHZ with 128 MB RAM and using Windows NT™ 4.0.

The flow chart 26 provided in figure 2 illustrates how the system 10 operates. As shown in block 28, the consumer initially establishes a connection over the Internet between the first computer 12 and the second computer 16 by accessing the on-line merchant's Web site using a commercially available browser, such as Internet Explorer™ or Netscape Navigator™. Then, as shown in blocks 30 and 32, using a GUI supplied by the on-line merchant, the consumer browses the on-line catalog, selecting which goods and/or services he wishes to purchase. Once the consumer makes his selection and is ready to place an order, the consumer transmits a purchase order message over the Internet to the on-line merchant (block 34).

The consumer is then prompted for his payment information, as indicated in block 36, which for purposes of the present discussion is an ATM card number and expiration date, although the payment information can include additional data such as the consumer's name and address. The consumer then transmits his payment information over the Internet to the on-line merchant, as indicated in block 38. As used herein, the term "ATM card" includes bank cards, debit cards and any other cards for which the issuing bank or organization may

require a valid PIN for use. The payment information is transmitted over the Internet using an encrypted connection, such as 128-bit encryption SSL.

When the on-line merchant receives the ATM card number, or earlier, the second computer 16 creates a unique session identifier by combining the consumer's IP address, which uniquely identifies the consumer, with a date/time stamp. The ATM card number is then forwarded, or echoed, over the Internet by the second computer 16 to the third computer 20 at the third party contractor location 22 (block 40), along with the unique session identifier, a merchant id which uniquely identifies the on-line merchant, a terminal id which identifies the terminal being used by the on-line merchant, the expiration date of the ATM card and the purchase price. This data package is stored in memory on the third computer in a queue. Once again, 128-bit encryption SSL is preferably used.

The data package transmitted by the second computer 16 to the third computer 20 is transmitted in ISO 8583 format. ISO 8583 is a messaging standard established by the International Standards Organization for financial transaction card oriented messages which is used by all banks and credit card companies and which is well known to those of ordinary skill in the art. A sample computer program written in Java which creates the unique session identifier and formats the data package in ISO 8583 format is provided in figure 5. This program is designed to run as an Active Server Page on Internet Server 4.0 under Windows NT 4.0, although the program can be used on other platforms and programming environments, and can readily be implemented by one of ordinary skill in the art.

Simultaneously or soon thereafter, the second computer executes a hyperlink to the third computer and the consumer is prompted by the third computer to input his PIN (block 42). The consumer inputs his PIN into the first computer 12 and transmits it over the Internet

to the third computer 20 (block 44). The connection between the first computer 12 and third computer 20 is encrypted and independent of the connection between the first computer 12 and the second computer 16 so that the on-line merchant is never in possession of the PIN. As with the second computer 16, the first computer 12 transmits the unique session identifier, the merchant id, the terminal id, the expiration date of the ATM card and the purchase price to the third computer 20 along with the PIN in a data package.

Figure 3 shows a typical GUI 46 which may be supplied by the third-party contractor and which pops up on the consumer's screen to allow the consumer to enter his PIN and transmit it to the third party contractor. As is clear from figure 3, the GUI 46 emulates an actual ATM machine and includes a simulated key pad 48 and a screen 50. The screen 50 indicates the on-line merchant's name and mailing address 52 and the purchase price 54. Using his mouse, the consumer inputs his PIN, as shown by the series of dots 56. By pressing the SUBMIT button 58, the PIN number is transmitted to the third party contractor. If the consumer makes a mistake, he presses the CLEAR button 60 and re-types his PIN. If the consumer needs help from the third party contractor, he simply presses the HELP button 62, which causes a help menu provided by the third party contractor to pop up on the screen, which may then be navigated by the consumer.

The third computer 20 next verifies that the ATM card number and PIN are valid (block 64). Because the third-party contractor may be overseeing multiple transactions at any given time, the third computer 20 must synchronize the data packages received from the first and second computers 12, 16. To do this, the third computer 20 matches the unique session identifier, the merchant id, the terminal id, the expiration date of the ATM card and the purchase price fields contained in the data packages received from the first and second

computers 12, 16. A sample computer program for synchronizing the messages received from the first and second computers 12, 16 is provided in figure 6. The program is written in C++ and can readily be implemented by one of ordinary skill in the art. All of the forgoing data fields must match in order for the transaction to take place. For security reasons, a two minute window for matching is preferably implemented. If there is no match within the two minute window, the transaction is aborted.

Once the data packages from the first and second computers 12, 16 are synchronized by the third computer 20, the third computer checks the ATM card number and PIN. If the ATM card number and PIN are invalid, the third computer 20 so informs the second computer 16 and the on-line merchant rejects the purchase order and notifies the consumer (block 66). If the ATM card number and PIN are valid, the third computer 20 checks to see whether there are sufficient funds to cover the purchase price 56 (block 68). If there are sufficient funds in the account, the third computer transmits an authorization message to the second computer, debits the consumer's account, the purchase is completed and the consumer is notified (block 70). If there are insufficient funds, a rejection message is transmitted, the on-line merchant rejects the purchase and the consumer is notified (block 72).

If the ATM card was issued by the third party contractor, the verification steps (blocks 64 and 68) may be done by simply accessing an internal database in or connected to the third computer 20. If, however, the ATM card was issued by another bank, then the third party contractor must verify the card information by contacting the issuing bank, either directly over a secure line, through a private ATM network, such as CIRRUS, or through any other available avenue.

The present invention is briefly and concisely summarized in figure 4. First, the consumer (first computer) transmits his ATM card number over the network to the on-line merchant (second computer) (block 74). Second, the on-line merchant forwards the ATM card number over the network to the third party contractor (third computer) (block 76). Third, the consumer transmits his PIN over the network to the third party contractor (block 78). As figure 4 indicates, the on-line merchant is completely bypassed and never receives the PIN. Fourth, the third party contractor verifies the ATM card number and PIN and checks for sufficiency of funds (block 80). Fifth, the third party contractor transmits the results of the verification process over the network to the on-line merchant (block 82). And sixth, the on-line merchant forwards the results over the network to the consumer, either completing or rejecting the purchase, depending on the verification results (block 84).

Thus, in accordance with the foregoing the objects of the present invention are achieved. Modifications to the present invention would be obvious to those of ordinary skill in the art, but would not bring the invention so modified beyond the scope of the appended claims.